REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicant thanks the Examiner for carefully considering this application.

Disposition of Claims

Claims 1-33 are currently pending in this application. Claims 10, 11, 16, 18-20, 26, 27, 29, 30, 32 and 33 have been canceled by this reply. Claims 1 and 21 are independent. The remaining claims depend, directly or indirectly, from claims 1 and 21.

Objections

Claims 6-20 and 24-31 have been objected to by the Examiner for multiple dependencies. Claims 10, 11, 16, 18-20, 26, 27, 29, and 30 have been canceled by this reply. Thus, this objection is now moot with respect to the canceled claims. Claims 6-9, 12-15, 17, 24-25, and 31 have been amended such that they no longer contain multiple dependencies. Accordingly, withdrawal of this objection is respectfully requested.

The Specification is objected to for an abstract of the disclosure that does not comply with 37 C.F.R. 1.72(b). A replacement abstract is provided with this response on a separate sheet. No new matter is added by way of the replacement abstract. Accordingly, withdrawal of this objection is respectfully requested.

Rejections under 35 U.S.C. § 112

Claims 32 and 33 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite. Claims 32 and 33 have been canceled by this reply. Thus, this rejection is now moot with respect to claims 32 and 33. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 102

Claims 1-5, 21, and 22 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,907,618 ("Gennaro"). Independent claims 1 and 21 have been amended to clarify the present invention as recited. Specifically, independent claims 1 and 21 have been amended to recite that the encrypted data is communicated between a decoder and a portable security module. Support for these amendments may be found, for example, on page 1, lines 3-4 of the Specification. To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

The claimed invention relates to the communication of encrypted data between a decoder and a portable security module in a digital television system. One or more precalculated key pairs are stored in the memory of the decoder, where each key pair comprises a session key and an encrypted version of the same session key. The encrypted version of the session key is obtained using a transport key. The encrypted value of the session key is communicated to the portable security module, which decrypts the value using the transport key stored in the memory of the portable security module. Thus, subsequent data that is communicated between the decoder and the portable security module is encrypted and decrypted using the session key that both the decoder and the portable security module have.

Advantageously, the use of a precalculated stored pair of values avoids the necessity of having to provide an encryption algorithm with in the decoder to encrypt an internally generated session key. Thus, the algorithm does not need to be a public/private key algorithm, but may be a symmetric algorithm.

In contrast to the claimed invention, Gennaro discloses a cryptographic key recovery system. Gennaro relates to a method and apparatus for verifying the correctness of key recovery information within a cryptographic key recovery system.

Turning to the rejection of the claims, for anticipation under 35 U.S.C. § 102, the reference must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. The Application respectfully asserts that Gennaro fails to anticipate the claimed invention for at least the following reasons:

> *(i)* Gennaro fails to disclose communication between a decoder and a portable security module in a digital television system. Those skilled in the art know that a decoder is a very specific type of device, used for the decoding of broadcast signals, for example, television and/or radio signals (*See* Specification, page 9, lines 1-5). The cited portion of Gennaro discloses a communication system for communication between a sender ("Alice") and a receiver ("Bob"), each using computer workstations to communicate. This is completely unrelated to encrypted communication in a digital television system between a decoder and a portable security module.
>
> *(ii)* Gennaro fails to explicitly disclose or suggest that the session key is used by a decoder and a portable security module to communicate, once the session key is decrypted by the portable security module using the transport key. In fact, because Gennaro fails to disclose communication of encrypted data between a decoder and a portable security module, it follows that Gennaro cannot possibly disclose the encrypted

communication between the decoder and the portable security module using a session key, as required by independent claims 1 and 21.

In view of the above, it is clear that Gennaro fails to disclose or suggest each and every limitation of the amended independent claims. Thus, amended independent claims 1 and 21 are patentable over Gennaro. Further, dependent claims 2-5 and 22 are patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claim 23 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro in view of U.S. Patent No. 5,835,726 ("Shwed"). To the extent that this rejection may still apply to the amended claims, this rejection is respectfully traversed.

As described above, Gennaro fails to disclose or suggest the limitations required by amended independent claim 21. Further, Shwed fails to supply that which Gennaro lacks. In particular, Shwed relates to controlling the inbound and outbound data packet flow in a computer network, thereby securing private networks from outside attacks and controlling to flow of packets within the private network to the outside world (*See* Shwed, Abstract). Shwed fails to disclose or suggest encrypted communication between a decoder and a portable security module in a digital television system. In fact, Shwed clearly relates to computer networks, and not digital television systems, and would therefore have no reason to disclose encrypted communication between a decoder and a portable security module using a common session key.

In view of the above, it is clear that independent claim 21 is patentable over Gennaro and Shwed, whether considered separately or in combination. Dependent claim 23 is patentable for at least the same reasons. Accordingly, withdrawal of this rejection is respectfully requested.

Conclusion

Applicant believes this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 11345.034001).

Dated: September 7, 2005

Respectfully submitted,

By #45079
Jonathan P. Osha THOMAS SCHERER
Registration No.: 33,986
OSHA · LIANG LLP
1221 McKinney St., Suite 2800
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Applicant

114832_1.DOC